REMARKS

Please reconsider the application in view of the following remarks.

Additionally, the Applicant notes that the formal drawings have not been acknowledged by the Examiner. Acknowledgement of the formal drawings is respectfully requested in the next Action.

I. Disposition of Claims

Claims 22-25, 27-28, 47-50, 52-53, and 57 remain pending in the application, with claims 22, 47, and 57 being the independent claims.

II. Rejections under 35 U.S.C. §103

Claims 22-25, 27-28, 47-50, 52-53, and 57 were rejected under 35 U.S.C. 103(a) as unpatentable over U.S. Patent No. 5,625,693 (hereinafter "Rohatgi") in view of U.S. Patent No. 6,014,723 (hereinafter "Tremblay"). This rejection is respectfully traversed.

The Claimed Invention

The claimed invention generally relates to a method of downloading data to an MPEG receiver/decoder. In another aspect, the claimed invention relates to a MPEG receiver/decoder configured to download data.

As recited in claim 22, the claimed invention includes, for example, the following steps:

A. a signature for the data to be downloaded is generated,

B. the signature and other data is included in a block of data with a selected offset between the start of the data block and the start of the signature,

C. the data block is encrypted using a private key,

D. the data to be downloaded and the encrypted data block are formatted as an MPEG table,

E. the MPEG table is transmitted,

F. the MPEG table is received,

G. the encrypted data block in the received MPEG table is decrypted using a public key corresponding to the private key,

H. at least one stored offset is looked up in a protected area of memory of the receiver/decoder,

I. the signature is extracted from the decrypted data block using the looked-up offset,

J. a signature is generated for the data in the received MPEG table, and

K. the generated signature is compared with signature extracted from the decrypted data block.

In the claimed invention, the offset is selected before the encryption takes place. Selecting the offset before encryption may be particularly advantageous, insofar as the using the

offset before encryption ensures that the signature is more difficult to find, since a potential hacker cannot identify the location of the signature within a data block.

Rohatgi

With respect to Rohatgi, Rohatgi teaches an apparatus and method for authenticating applications transmitted over an interactive TV system. Rohatgi includes the following steps:

a. a signature for the data (*i.e.*, the module, col. 8, lines 45-49) to be downloaded is generated,

b. the signature and other data is attached to the block of data (*i.e.*, the module, col. 8, lines 45-49),

c. the data block is encrypted using a private key (col. 8, lines 45-49),

d. the encrypted data block is divided into transmission units (TUs), each of which has a header with a module TU byte offset (Figure 4),

e. the TU is transmitted,

f. the TU is received,

g. the payload of the TU is extracted using the module TU byte offset,

h. the encrypted module is decrypted using a public key corresponding to the private key,

i. the signature is extracted from the decrypted data block,

j. a signature is generated for the data in the received MPEG table, and

k. the generated signature is compared with signature extracted from the decrypted data block.

From the above, it can be understood that the steps of Rohatgi generally correspond to the steps A, C, E, F, J, and K of the claimed invention. However, steps B, D, G, H, and I of the claimed invention require further scrutiny.

First, with respect to step B, the present invention includes the signature in a block of data with a selected offset between the start of the data block and the start of the signature, but Rohatgi is completely silent to this feature. In fact, Rohatgi takes the "hash" value and either attaches the hash value to the hashed module or puts it in the Directory Module (which may be further hashed, encrypted *etc.*) Thus, with respect to step B, Rohatgi does not use any kind of offset before encryption.

As for step D, the encrypted data block is formatted as an MPEG table in the claimed invention. However, Rohatgi divides his data block (*i.e.*, the module) into transport units (TUs), where each TU has a module TU byte offset. It is important to note that this TU byte offset is completely different from the present invention, because the TU byte in Rohatgi is used after encryption. As previously mentioned, using the offset before encryption makes the signature much more difficult to find, since a potential hacker cannot identify the location of the signature within a data block. However, offsetting after encryption does not provide the same enhancement of security.

Finally, with respect to steps G-I of the claimed invention, these steps generally relate to the "decryption" and, thus, correspond roughly to steps B and D in the reverse order. Particularly, in the present invention, the encrypted data block is decrypted and the offset is looked up and used to extract the signature.

On the other hand, Rohatgi extracts the payload using a public key (which corresponds to a private key), decrypts the module, and performs a straightforward extraction of the signature. As acknowledged by the Examiner, Rohatgi does not teach looking up the offset in a protected memory after decryption to extract the signature. This is not surprising, as the offset in Rohatgi is not used in the same manner as the offset of the present invention.

As previously discussed, Rohatgi does not teach all of the elements of the present invention. Tremblay fails to provide that which Rohatgi lacks. Further, Tremblay was combined with Rohatgi solely to show a "looking up the offset stored in the memory area of the receiver/decoder." However, Tremblay fails to teach a method of downloading data to a MPEG receiver/decoder, such that "the signature and other data is included in a block of data with a selected offset between the start of the data block and the start of the signature," prior to encryption, as recited in claim 22.

One skilled in the art will appreciate that the combination of Rohatgi and Tremblay do not teach the present invention. The combination, assuming *arguendo* that the combination is properly motivated, would simply not perform the steps of the claimed invention in the proper sequence. Further, since this sequence is important to the function of the present invention, namely, selecting an offset after encryption versus selecting an offset before encryption, Rohatgi and Tremblay fail to teach the present invention. Thus, claim 22 is patentable over Rohatgi and

Tremblay, whether considered separately or in combination. Claims 23-25, 27, 28, 47-50, 52, 53, and 57 are also patentable for at least the same reasons.

III. Conclusion

Applicant believes no fee is due with this response. However, if a fee is due, please charge our Deposit Account No. 50-0591, under Order No. 11345/107001 from which the undersigned is authorized to draw.

Dated: 9/17/04

Respectfully submitted,

By for Jonathan P. Osha 48,885

Registration No.: 33,986
OSHA & MAY L.L.P.
1221 McKinney St., Suite 2800
Houston, Texas 77010
(713) 228-8600
(713) 228-8778 (Fax)